This document contains excerpts from the X-34 Independent Assessment Report (title page shown below). Only those sections which relate to the PBMA element **Operations** are displayed.

The complete report is available through the PBMA web site, Program Profile tab.

X[34]

Safety & Mission Assurance Review

NASA
Office of Safety & Mission Assurance

June 17, 1998

2.6 Range and Facilities

White Sands Missile Range is a multi-service test range whose main function is the support of missile development and test programs for the Army, Navy, Air Force, NASA, other government agencies and private industry. The White Sands range is under operational control of the U.S. Army Test and Evaluation Command (TECOM), Aberdeen Proving Ground, Maryland. TECOM is the Army's test laboratory for planning and conducting engineering and service tests of all materials from missiles to rifles, tanks to trucks, clothing to radios, and from aviation to fire control equipment. Holloman Air Force Base is located in the south-east corner of the WSMR and provides the pre-launch processing support for the L-1011/X-34 flight system.

White Sands Missile Range is in the Tularosa Basin of south-central New Mexico. The range boundaries extend almost 100 miles north and south and 40 miles east to west. At 3,200 square miles the range is the largest military installation in the country and could easily encompass the states of Delaware and Rhode Island. The headquarters area is 20 miles east of Las Cruces, New Mexico, and 45 miles north of El Paso, Texas. Additional call-up areas are lands either privately owned or controlled by state and federal agencies. White Sands has contracts with ranchers in these areas which allow the range to evacuate the residents for up to 12 hours a few times a year for some tests. The ranchers are paid a yearly payment and travel expenses each time they evacuate. When utilized, the call-up areas add about 2,500 square miles for the range's temporary use. The only area regularly open to the public is the main post where there is a museum, missile park and White Sands National Monument.

White Sands Missile Range has more than 1,500 precisely surveyed instrumentation sites and over 1,000 of the newest and most modern types of optical and electronics instrument systems. These include long-range cameras, tracking telescopes, interferometer systems, radars, and telemetry. For general use, radars, telemetry, and optic systems include both mobile and fixed systems. A timing system provides fixed-timing rates, elapsed time, and control signals. Control signals are combined into pulsed signals in standard format for distribution and utilization. Other range services include calibration, communication, meteorological, photographic, television and aerial target support along with the relatively easy and fast recovery of test items which facilitates evaluation.

3.4 Operational Safety (System Safety & Range Safety) Processes

3.4.1 Requirements

As discussed in Section 2.0, OSC will implement the baseline flight test program from the White Sands Missile Range/Holloman Air Force Base (HAFB) complex near Las Cruces, New Mexico. All operations will be conducted over the WSMR. The OSC Flight Assurance manager is responsible for coordinating or orchestrating the ground and flight safety activities related to the X-34 vehicle.

X-34 flight operations are governed by the WSMR Base Commander and the national range universal documentation system. The Range Safety Process is under the control and direction of the Base Commander. The Range Safety Office is responsible for all issues regarding Flight Termination System (FTS) design reliability and redundancy, as well as FTS command-destruct and communication system security.

System Safety & Range Safety Requirements

- X-34 Accident Risk Assessment Report (ARAR), (TD-9110, Rev X2.), contains technical information concerning hazardous and safety critical equipment, systems, and materials used in the X-34. This document is prepared for WSMR Range Safety and HAFB Safety to Review, and will be submitted to WSMR Range Safety and HAFB Safety prior to hardware shipment.
- The ARAR will provide in detail the L-1011/ X-34 hazards.
- The Flight Termination System Report, (TD-9111), provides a detailed flight termination system description, hardware, and test reports.

OSC System Safety Requirements

- Flight systems shall satisfy all negotiated range safety requirements associated with WSMR, HAFB and FAA as required in the following documents:
  - X-34 Design Safety Requirements Document, X60023
  - X-34 Safety Requirements for Ground Operations, X60024
- Flight systems shall be two fault tolerant to any catastrophic event
- No single credible failure or operator error during ground operations shall result in significant personnel Injury or damage to flight hardware.
- X-34 vehicle shall be safe to jettison from L-1011.
- A function whose inadvertent operation could result in a catastrophic event must be controlled by a minimum of three inhibits, whenever the potential exists. At least two of the three required inhibits are monitored.

Hazard Analysis Ground Rules

For purposes of the Hazard Analysis, the carrier aircraft is considered part of the X-34 flight system. A catastrophic event is defined as either:

- catastrophic damage to carrier aircraft or ground facilities, or
- personnel death.

Catastrophic Damage to the carrier aircraft or ground facility is defined as damage that results in total loss of flight worthiness of the carrier aircraft or major facility damage. Credible failure is a condition that can occur and is reasonably likely to occur. Failures of structure, pressure vessels, and pressurized lines and fittings are not credible if they comply with appropriate design margins of safety.

3.4.2 Ground Operations

X-34 pre-flight ground operations take place at HAFB. HAFB provides necessary ground support equipment and implements the OSC ground safety program contained in "Safety Requirements for Ground Operations" X60024. The loading of both liquid oxygen and RP-1 is carried out by WSTF personnel. The NASA White Sands Test Facility, operating under an OSC task agreement, provides LOX safety support.

3.4.3 Captive-Carry Operations

Captive-carry is the term used to describe the mated L-1011/X-34 vehicle. This aerospace flight system must be certificated by the Federal Aviation Administration (FAA) as an experimental aircraft and must demonstrate compliance with applicable Federal Aviation Regulations (FAR's). OSC has retained the services of Marshall Aerospace Ltd. to perform the necessary work to acquire FAA certification. OSC has established a task agreement with NASA Dryden Flight Research Center to conduct the flight testing necessary to demonstrate compliance with FAA requirements.

<u>L-1011/X-34 Aerodynamic Separation Analysis and Verification</u>

Separation Modeling

L-1011/X-34 separation analyses have been completed for the first flight scenario involving drop of the unfueled/unpowered 18,000 lb. vehicle. Analysis and testing continues in preparation for the fueled-powered flight scenarios.

The static vertical margin is 17 inches between the X-34 rudder tip and aft end of the L-1011 fin box. The static horizontal margin between the X-34 rudder and the L-1011 fin box is four inches. Analyses by Nielsen Engineering and Research (NEAR), Palo Alto, California, provided guidance for selecting the optimal drop condition which gives the most clearance margin. OSC conducted independent analyses which verified (and extended) the NEAR assessment. The NEAR aerodynamic model developed for the jettison of munitions ("stores model") has been used successfully to model the drop of the Pegasus air-launched expendable launch vehicle.

X-34 Roll Mitigation at Drop

The X-34 roll autopilot is being used at the time of drop so as to avoid side impact of the rudder given the limited clearance available. Simulations indicate that all lateral (static lateral clearance minimum is 4 inches) impact cases are avoided with the use of the X-34 roll autopilot. Limited impact cases may exist for a roll autopilot failure, however the impact forces calculated would not cause damage to the L-1011 fin box.

Wind Tunnel Testing

A separation wind tunnel test is scheduled for July 27, 1998 in the Calspan (formerly the Cornell Aeronautics Laboratory) transonic wind tunnel located in Buffalo, New York. 1/30th scale L-1011 and X-34 vehicle models will be tested to determine the captive carry and close proximity flow field. The data will be used to run further simulations and build confidence in the nominal separation conditions and drop envelope. Wind tunnel data for control surface deflections corresponding to multiple failures will be gathered to estimate impact forces. At this time the system is two fault tolerant to a control surface hardover at the time of drop. Multiple failures or "non-credible " control surface hardovers are only being given limited evaluation since the probability of their occurrence is very small. NASA Langley Research Center is assisting in test scenario definition, testing and data reduction.

X-34 Propellant and Oxidizer Slosh Mitigation and Analysis

In discussions during the on-site review questions were raised concerning the influence of sloshing partial-fuel-load forces on L-1011/X-34 separation margins. All tanks incorporate slosh baffles to minimize the amount of slosh during flight operations.

No scenarios currently exist in which the X-34 has a partially full RP-1 tank during captive carry operations. Maintaining a full RP-1 tank is also a requirement for (non-launch) point to point transportation across U.S. In the case of liquid oxygen (LOX), a maximum boil-off of 6% is allowed. At the time of drop, the LOX tanks will be between 94 and 100% full. Therefore LOX sloshing could occur if the L-1011/X-34 flight system is accelerating (climbing, descending turning). Current flight rules require the flight system to be stable for approximately 10 minutes prior to drop, imposing no acceleration on propellant or oxidizer. Follow-on discussions with OSC indicate that slosh could possibly be a factor in an emergency jettison scenario where the flight system is not trimmed and stable. It is recommended that OSC consider the emergency release scenario where the L10-11 is maneuvering and LOX boil off has created a 94% LOX load and associated slosh to assure that forces associated with sloshing will not influence separation margins.

Safety Hazard Analysis

During the baseline flight test program, all failure modes of the L-1011/X-34 vehicle will be contained within the bounds of the WSMR. It is important to note that any potential operations from the Eastern Range (OPTF) will require consideration of complex abort scenarios which will require over-flight of populated areas.

In addition to the flight assurance gained through FAA certification, OSC has in-place a corporate level flight system safety directive, which identifies and evaluates safety hazards to the flight crew and technical staff on board to OSC L-1011. These analyses are contained in the ARAR. Development of this document involves development of

Failure Modes and Effects Analysis (FMEA), Fault Tree Analysis, and Hazards Analysis. Selected ARAR examples follow:

- Premature Engine Ignition While In Captive Carry

  Hazard
  - Engine ignition while attached to the L-1011 will cause catastrophic damage and loss of life

  Control Features
  - 2 utility controller inhibits : breakwire and firing Field Effect Transistor
  - 3 monitored inhibits in the Flight Termination Logic Unit (FTLU), breakwire-dependent, with a 2.5 second time delay for safe separation distance.

  Verification
  - functional testing
  - FTLU and utility controller inhibits are monitored by Launch Panel Operator (LPO)

- Premature Engine Ignition After Release Prior To Safe Separation Distance

  Hazard
  - X-34 engine ignition prior to safe separation distance from the L-1011 will cause catastrophic damage

  Control Features
  - FTLU has a 2.5 second time delay for safe separation distance prior to enabling engine ignition relay
  - Flight computer needs to sense breakwire prior to starting flight portion of Mission Data Load
  - Inertial Navigation System (INS) velocity and attitude must be within proper limits.

  Verification
  - Functional testing
  - FTLU and utility controller inhibits are monitored by LPO prior to release

- Parachute Deployment While In Captive Carry

  Hazard
  - Parachute deployment while in captive carry could result in L-1011 damage or loss of control

  Control Features
  - Design is inherently safe. Capture pin must be engaged for chute to be structurally coupled to X-34. Capture pin is not engaged during captive carry
  - Flight computer and utility controller inhibits

  Verification
  - System functional testing

- Flight computer breakwires and utility controller inhibits monitored by LPO and ground controllers.

- Landing Gear Deployment While In Captive Carry

  Hazard
  - Landing gear deployment while in captive carry could result in L-1011 loss of control and prohibits safe separation of X-34. L-1011 can not safely land with X-34 landing gear deployed

  Control Features
  - Flight computer and utility controller inhibits
  - Launch panel operator (located on L-1011): hydraulic isolation valve isolates the X-34 landing gear from the hydraulic system

  Verification
  - System functional testing
  - Flight computer breakwires and utility controller inhibits monitored by LPO and ground

These examples have been specifically selected to highlight the captive-carry and separation risk issues raised in discussions during the on-site review meeting.

3.4.4 Flight Operations

WSMR Range Safety Management Documentation

The principal WSMR range safety requirements document is "NROCE-991-001 Rev. 1, Flight Termination System (FTS) Requirements Document For The X-34 Technology Test Bed Vehicle." This document, tailored from Range Commanders Council (RCC) 319-92, sets forth the WSMR Range Safety requirements for the X-34 technology test bed vehicle FTS. It outlines the requirements for establishing design criteria, testing, and data submittals. It also prescribes the procedures for FTS flight test approval, approvals of subsequent modifications, and defines the operational authorities and responsibilities. The Safety Engineering Branch (STEWS-NRO-CE), Operations Control Division, National Range Operations Directorate, WSMR, is the range element responsible for resolving problems associated with design, usage, and test of the FTS at the missile test range.

The identified policies, requirements, and procedures are binding upon the X-34 test program at WSMR, unless specifically amended or waived, in writing, by the Commanding General of WSMR, or his duly authorized representative. The X-34 Program Office, or its duly authorized contractors, are responsible for fulfilling the requirements specified. The compliance with this document does not guarantee the acceptance of the X-34 FTS at other ranges.

Range FTS Approval Process

The Range FTS approval process is a five-phase approach in which; (1) the program requirements are identified, (2) an FTS concept is derived which meets program and range safety requirements, (3) a final FTS design is made which functions as per the concept, (4) the design is qualified for use through a series of design verification tests, and (5) the FTS is approved for use at the Range following the approval of all operational, test, and checkout procedures.

FTS approval must be obtained 60 days prior to the start of flight test operations. This approval will be granted following satisfactory fulfillment of the requirements specified herein. Satisfactory performance in these requirements is determined by the WSMR Safety Engineering Branch, (NRO-CE). Participation by this organization during all phases of the concept, design, approval, qualification testing, pre-test, vehicle build, ground pre-test and flight test is required. Level of Range participation in these activities will be determined by the Range. After approval, continued coordination must be maintained to ensure that any modifications still result in an approved FTS for use at the Range.

The following is a summary of the requirements that the X-34 will have to meet prior to gaining approval:

FTS Reliability

The overall FTS reliability must be demonstrated. The overall system reliability of the FTS shall be 0.999 with a 95% confidence level. FTS reliability may be demonstrated by meeting the following four requirements:

- Designing the FTS to be fault tolerant.
- Performing Range approved qualification, acceptance, certification, and pre-mission testing.
- Maintaining stringent quality control as required by MIL-STD-973, *Configuration Management,* 24 Nov 93, reference 2.2h, or other acceptable quality control specification agreeable to the Ranges.
- Performing a reliability prediction on the FTS to show the 0.999 probability is met. The mission time used in the reliability predictions shall include a minimum of 150% of the predicted flight time and shall be verified by analysis in accordance with the Parts Stress Analysis of MIL-HDBK-217E, *Reliability Prediction of Electronic Equipment*, reference 2.3, using the applicable environmental factor.

Flight Termination System Report (FTSR)

To obtain final FTS approval by the Range, and prior to the first vehicle flight, the user must provide a final FTSR that contains the following data items:

- A detailed narrative description of the FTS;
- Detailed FTS schematics and wiring diagrams;
- FTS component specifications;
- QA procedures and reliability documentation;
- Antenna patterns;
- Link Analyses;
- Battery Load Analyses;
- Environmental Analyses;
- Bent-Pin Analyses;
- FMECA;
- Qualification test plans/procedures/reports;
- Acceptance test plans/procedures/reports;
- Failure analyses reports (if applicable);
- Certification test procedures/reports;
- FTS assembly and checkout procedures;
- Modifications (if applicable);
- Waivers granted (if applicable).

FTS Design Configuration

The FTS shall be redundant to the maximum extent possible, and shall include the following components; Dual UHF flight termination receivers (FTRs), FTS antennas and coupler, independent, redundant FTS battery power system, redundant independent Flight Termination Logic Units (FTLU), appropriate end items, circuitry interconnecting these components, and the control/monitoring circuitry and equipment.

- Independence. The FTS shall be independent of all other vehicle systems except where agreed upon by the Range.

- Accessibility. The FTS circuitry shall be configured to be field testable requiring minimum disassembly. Design should accommodate easy replacement of FTS components where such is likely to be required.

X-34 FTS Performance Characteristics

The FTS must be able to be activated by:

- A commanded signal which engages a prescribed sequence of modulating Inter-Range Instrumentation Group (IRIG) tones.
- The FTS Action 1, must result in shutdown of the vehicle main propulsion unit.
- The FTS Action 2, must result in placing the vehicle into an unstable attitude which produce zero lift, zero yaw, and zero thrust.
- These actions, shall be independent and configured to afford their usage at the discretion of the Range Safety Officer.

Pre-Flight Readiness Review Process

The following reviews will be conducted prior to each flight:

- Flight Safety Review (L-2 to L-4 weeks)
    - Finalize WSMR Flight Safety Operational Plan
    - Flight safety oriented
- Mission Readiness Review (schedule TBD)
    - Vehicle preparedness
    - Mission success oriented
- Flight Readiness Review (L-1day)
    - Range preparedness

These reviews are a sub-set of the overall X-34 program review process described in Section 3.2.8 of this report.

Between-Flight Safety Assurance Processes

The integrated vehicle health monitoring system, which, together with rapid software reprogramming, will make possible the quick turnaround of the X-34 vehicle. As previously noted, this is a major demonstration goal.

The philosophy for accomplishing turnaround validation/checkout is to evaluate vehicle performance via telemetry information and generate any required Field Discrepancy Reports (FDR's) based on this data. The FDR is used to document troubleshooting, and, in conjunction with existing procedures, to remove and replace hardware. In addition, a visual inspection of the vehicle external surfaces, and internal cavities will be performed and discrepancies and repairs documented in FDR's.

Operations will perform functional testing at the subsystem level following vehicle maintenance and repairs during each turnaround. This functional testing will be performed as a "Vehicle Verification" test which will use the flight computer to verify the functionality of each avionics, hydraulics, pneumatics, and MPS component on the vehicle. In effect, if the avionics system interfaces with a component, then that interface and the functionality of the component is verified. The remainder of the hardware will be serviced on a periodic basis. The selection of periodic validation/checkout intervals will be through subsystem/hardware analysis results, failure history, and the disposition and corrective action implementation of prior failures. The X-34 structural and subsystem inspection task will be performed each turnaround or until a damage tolerance has been developed to satisfy the program. The major forms of damage considered during the initial phase of the program are:

- Fatigue/Dynamic load damage
- Environmental deterioration or damage
- Accidental damage
- Thermal Damage or degradation

Software will be validated by "hardware in the loop" testing following any modification to the flight software load.

The FASTRAC engine will be removed after each powered flight. Contamination control measures to be defined by the MSFC/FASTRAC engine program will be implemented to protect the main propulsion system plumbing, valves and tanks. It is anticipated that a positive pressure purge method will be employed. NASA WSTF (under a task order agreement with OSC) will be defining the LOX servicing/contamination prevention requirements that would be implemented between flights. Installation of a new engine will be conducted in accordance with MSFC/FASTRAC engine program defined requirements.

<u>Payload Safety Review Process</u>

Payload safety is governed by X-34 project documents X60023 and X60024. These requirements include pre-ship payload safety reviews as well as a formal payload hazard analysis. The review board is chaired by the X-34 Flight Assurance manager.

3.4.5 Range Safety Working Group

OSC Flight Assurance Manager and the WSMR Range Safety Officer co-chair this working group. This team conducts weekly telecons and provides a forum to identify, document and track work items necessary to fulfill range safety requirements. An example from the Range Safety Working Group Log is shown below.

3.4.6 Emergency Response Planning Process

WSMR and HAFB require that a emergency response plan be developed for all tests. OSC plan addresses emergency situation during ground, flight, and test operation. Test coupons of the composite structure will be burn tested to obtain additional information concerning hazards associated with smoke. This information will be included with the Material Safety Data Sheets (MSDS) to represent the greatest hazard chosen and used to represent the entire vehicle. Training will be provided to WSMR and HAFB crash and fire rescue personnel by OSC for familiarization with X-34 and location of hazardous components. Existing training course for the L-1011 safety will be conducted by the L-1011 Flight Engineer with safety and emergency response personnel at HAFB, WSMR, and NASA White Sands Test Facility (WSTF) following the L-1011 arrival for the first flight. Contingency procedures will be modified to include the L-1011 with X-34 attached. Lesson learned from the NASA, DC-XA, Clipper Graham mishap contributed to the development of this plan.

4.0 X-34 Safety & Mission Assurance Issues

4.1 System Safety

Flight safety issues were discussed at length during the on-site review. It can be expected that continuing and expanded SMA insight will be required as the program moves to the optional flight test program.

Heritage Software Concerns

It noted that while L-1011/Pegasus heritage supports the development of captive-carry hazards analyses and extreme care should be used to avoid over-reliance on this heritage, as the X-34 represents a new and unique configuration.

Flight Safety During Captive Carry Operations

Questions have been raised concerning L-1011/X-34 catastrophic failure modes including premature or inadvertent drop during captive carry, post separation collision, and premature engine ignition. OSC and MSFC SMA must maintain a high level of rigor in documenting analyses and testing necessary to support development of risk acceptance rationale.

FAA Certification of L-1011/X-34

Increased insight is required (on the part of NASA) to better understand the processes involved in FAA Certification of L-1011/X-34. Marshall Aerospace Ltd. is under contract to OSC to acquire FAA certification. DFRC is the subcontractor to OSC to manage FAA certification testing. The NASA FASTRAC engine program is on the critical-path to furnish information necessary to acquire certification. Difficulties have been encountered over the past six months in communicating required data in a timely fashion. Issues have also been raised concerning how OSC will demonstrate compliance with pressure vessel safety requirements necessary to satisfy Federal Aviation Regulations (FARs). OSC is using Mil Standard 1522 as the standard for X-34 pressure systems to meet FAA certification requirements, (although FAA does not specifically require compliance with Mil Standard 1522). OSC has also indicated concern with traceability and insight into the FASTRAC engine development. NASA and OSC managers must better communicate and coordinate on issues related to FASTRAC safety and mission assurance.

4.3 Potential Eastern Range Operations

The X-34 program will face a variety of new and different requirements for operations off the U.S. east coast. For example, the Eastern-Western Range (EWR-127) requires parts traceability for FTS components while the WSMR does not impose this specific requirement. Hardware changes will be required. The X-34 will have a nominal mission trajectory that is completely within U.S. military coastal restricted areas, however, some east coast abort sites will involve overflight of populated areas. The environmental assessment process and the range safety hazard analysis will become more complicated (and more contentious). OSC will most certainly have to increase the X-34 Flight Assurance staff to accommodate the increased work load. NASA/MSFC SMA management should work to acquire insight into the advanced planning for the optional flight test program operations.

4.4 Baseline X-34 Flight Termination System (FTS)

X-34 Flight Termination System Hardware

OSC has purchased the FTS receiver from Herley-Vega (HV) as recommended by the White Sands Missile Range (WSMR). HV receivers have been in use at WSMR since 1990. While this receiver has a long record of demonstrated flight success, HV uses commercial manufacturing practices where parts traceability and documentation is not a standard service. Note that the absence of parts traceability may represent an issue for the certification of the HV-FTS on the Eastern Test Range because of EWR 127-1 requirements for 100% parts traceability.

X-34 Flight Termination Process

The X-34 flight termination process involves two steps. The first FTS up-link command, “engine cut-off”, closes the engine valves which shuts down the propulsion system. With engine shutdown the flight computer autonomously sends commands to dump remaining fuel and oxidizer. The X-34 continues to operate under autonomous internal guidance/navigation and control software and has the opportunity (5 to 8 seconds) to correct the errant trajectory. If the vehicle fails to recover, a “terminate” command is transmitted resulting in an “energy dissipation mode”, where there is no net lift, and the vehicle assumes a ballistic trajectory. This is accomplished by a high pressure helium system which simultaneously drives the port elevons (control surfaces) up, and the starboard elevons down.

4.5 Flight Termination System Communication Security Issues

The issue of inadvertent or intentional interference with FTS (and/or command and control up-link) has been raised in recent discussions with the NASA Inspector General (IG). This issue relates not only to the X-34 but to other X-vehicles and space flight programs.

The NASA Inspector General (IG) has recommended implementation of a high security FTS command/destruct decoder-initiator system and an equally secure command uplink system. Tampering, spoofing (jamming or misdirecting) or other intentional interference with the FTS could result in destruction of the vehicle during nominal operation or impairment of range safety’s ability to terminate flight in the case of an errant ground track.

Secure FTS

Command Receiver Decoder (CRD) receives signal, decodes signal, and initiates termination function. Ground-based Command Transmitter System (CTS) generates, modulates, and transmits the signal. Differences between secure and non-secure systems involve; 1) destruct command generation in the CTS, and 2) decoding of the destruct command on-board the vehicle. The IG indicated that a cost increase on the order of \$85K to \$120K would be associated with implementation of secure system hardware. Additional costs would be associated with program compliance with security control and handling requirements.

Range Safety and FTS Responsibilities

Acknowledging NASA and OSC's shared responsibility for assuring public safety, the military test range Base Commander nonetheless has ultimate responsibility for any vehicle launched from his/her facility. The Base Commander delegates range safety responsibilities to the Range Safety Office that addresses issues related to:

- Flight Termination System (FTS) hardware design
- FTS software
- Flight hazard and public safety

The X-34 program will need to work with the White Sands Missile Range Safety Office for operations in New Mexico, and the USAF, 45th Space Wing, for operations based at Kennedy Space Center. Range safety requirements for KSC operations are contained in EWR 127-1. Range safety requirements for WSMR are contained in RCC-319-92, and special RLV revision, NROCE-991-001 rev.1, "Flight Termination System (FTS) Requirements Document for the X-34 Technology Testbed Vehicle."

Scenario 1: The "Casual Hacker" Threat

Threat Scenario

This scenario presented by the IG involves an individual using the internet to discover information concerning the FTS manufacture and design specifications, including default tone settings. The non-secure FTS receiver has up to five tones available for identity/authentication access necessary to enable command. In reality only a two-tone code is typically employed.

The Casual Hacker could then acquire a relatively inexpensive (several hundred dollars) radio transmitter and associated hardware, (power supply etc.) and be capable of sending unauthorized commands and/or jamming or spoofing the FTS receiver.

Risk Mitigation

This potential threat was discussed with OSC avionics and operations Team Leads during SMA review background technical meetings on May 6 and 7, 1998. The following mitigation measures (already in place) were identified as more than adequately addressing the Casual Hacker scenario.

- Range frequency control officials at WSMR are continually monitoring all radio frequency (RF) transmissions in and around the WSMR. Any unauthorized transmission (on any frequency) would immediately be identified, located and addressed by security personnel. Any unauthorized transmission would cause the range to immediately assume a "Red" (cease operations) status.

- Range flight termination system receivers on the X-34 vehicle would not be turned on until the X-34 flight operations manager was instructed by the Range Safety Officer (RSO) to do so. Prior to issuing this clearance the RSO would confirm that the X-34 vehicle was "saturated" with RF radiation from the powerful range safety antenna system, radiating 600 to 1000 watts of RF power. This level of power will preclude the successful intrusion of a lower power level (unauthorized transmission) into the FTS receiver detector.

- Once "locked-up" by the range safety RF system the X-34 FTS receiver automatic gain control (AGC) and noise detection electronics would reject any lower wattage transmission on the FTS carrier frequency. It was described as a "signal-to-noise" struggle that range safety would always win.

- The X-34 FTS communication system will also provide a continual downlink of telemetry to the RSO, providing verification of FTS receiver RF saturation. In the event of anomalous receiver operation prior to drop, the range would immediately move to a "Red" status.

<u>Scenario 2: The Sophisticated "Bad-Guy" Threat</u>

Threat Scenario

This threat would involve RF attacks launched by a nation or organization capable of radiating hundreds or thousands of watts of RF power from an undisclosed/undiscovered location for presumed political purposes.

This scenario was discussed during the SMA review conducted earlier this year at the Lockheed-Martin Skunkworks facility near Palmdale California. Clear differences of opinion existed between the NASA IG communication security experts and the Edwards Air Force Base range safety personnel concerning the existence of a credible security threat to operations on the California/Utah/Montana test range.

Risk Mitigation:

Secure FTS system including receiver/decoder and up-link encryption provides the most obvious means of mitigating this threat scenario. In the case of the X-33, the review team and the X-33 program mutually acknowledged that additional mitigation measures (i.e., secure FTS system deployment) would be appropriate if a credible threat was present.

Resolution of X-34 Risk Management Issues Concerning FTS

The NASA OSMA review team recommends that the X-34 program management team should work with the NASA Office of Security (Code J), and the NASA Inspector General (Code W) to assess the need for a secure FTS system to support on-range, flight operations in New Mexico.

A separate risk management process (involving Code J, Code W, the KSC operations, and the US Air Force, 45th Space Wing) should be employed to address east coast operations involving a 2000 mile, off-shore, flight corridor, ranging from Wallops Island, Virginia, to Cape Canaveral, Florida. The east-coast scenario presents a different set of signal-to-noise ratio issues, with longer distances from range RF transmitters to the vehicle, and reduced abilities to control unauthorized RF emissions. While the Casual Hacker threat would be largely precluded by off-coast, long range operations it could be argued that a sophisticated attack scenario (assuming such a threat exists) using ship-based, high-power, RF transmitters would have greater opportunity to succeed.